defective; claims 1-18 were rejected as being based upon a defective reissue declaration under 35 U.S.C. § 251; claims 1-2, 6-7, 11-12, and 17-18 were rejected under 35 U.S.C. § 102(b); and claims 3-5, 8-10, and 13-16 were rejected under 35 U.S.C. § 103(a). Claims 1-18 are presented for consideration.

**Reissue Application**

The application was objected to under 37 C.F.R. § 1.172(a) due to the assignee not having established its ownership interest in the patent for which reissue is being requested. The enclosed statement under 37 C.F.R. § 3.73(b) establishes Fujitsu's ownership interest in the patent for which reissue is requested. Therefore, applicant requests reconsideration and withdrawal of the objection to the application under 37 C.F.R. § 1.172(a).

The Office Action stated that the reissue oath/declaration filed with the application was defective. Under M.P.E.P. § 1414.01, applicant will submit a supplemental reissue oath/declaration correcting the identified defects prior to allowance of the application.

Claims 1-18 were rejected as being based upon a defective reissue declaration under 35 U.S.C. § 251. As discussed above, the defects in the reissue declaration will be corrected prior to allowance.

**35 U.S.C. § 102(b)**

Claims 1-2, 6-7, 11-12, and 17-18 are rejected under 35 U.S.C. § 102(b) as being anticipated by *Matyas* (U.S. Patent No. 4,757,534). The Office Action asserts that *Matyas* discloses each and every element of the claimed invention.

Claim 1 recites a storage medium accessed by a vendor computer and a user computer. The storage medium stores information readable by the user computer. The storage medium includes encrypted electronic data. A medium personal number which is unique for each storage medium is provided where at least the medium personal number is written onto the storage medium in an un-rewritable form which the user computer cannot rewrite. The medium personal number is used for generating a decryption key for decrypting the encrypted electronic data in the user computer.

The present specification discloses a storage medium containing a medium personal number stored thereon. The storage of the medium personal number on the storage medium itself permits the storage medium to be used on more than one computer, but, on only one computer at a time. Consequently, an authorized user could, for example, utilize the storage medium on his computer in the office and then take the storage medium home and use the same storage medium on his or her home computer.

The Office Action asserts that *Matyas* discloses a software protection system for a storage medium (a diskette) accessed by a storage readable apparatus (a user computer). The protection system provides for a medium personal number unique to each storage medium written onto the storage medium in an un-rewritable form which a user storage readable apparatus cannot rewrite. See Figure 2 and 7 of '534 where the computer password (formed from the program and diskette serial number, see col. 5, lines 30-37) is indicated as "rewrite/overwrite not permitted by software". The computer password allows for generating a decryption key for decrypting the encrypted electronic data (as in claims 1-2) or generating an encrypted permission information (as in claims 6-7 and 11-12) or for decrypting the encrypted electronic information which is encrypted based on the medium personal number (as in claims 17 and 18).

In contrast, it appears that *Matyas* teaches a software protection system for a storage medium (a diskette) accessed by a user's computer. In order to utilize the program on the diskette, the user must first obtain an authorization number and a password from the software vendor. The password allows the encrypted program to be recovered at the prescribed, designated computer 10 having a properly implemented and initialized encryption feature. Both the authorization number and password are required for the particular program to be decrypted and executed. Both the authorization number and password are unique to the particular program and computer where the program is to be executed. Each diskette has a unique serial number written on the diskette envelope or outer cover and is visible to the user. The serial number is also recorded in the header record of the diskette together with the program number. The authorization number is obtained by encrypting the program number and the diskette serial number under a secret cryptographic key available to or known only by the software vendor. Consequently, after purchasing the program, the user places a telephone call to the software vendor. The user provides the software vendor with the program number, the n-bit portion of the authorization number, the diskette serial number, and the user's computer number. The identification number for the computer is associated with the secret key of the crypto facility of the computer. Thereafter, the vendor combines a disk number and the program number to generate an authorization number. The authorization number is then compared with the n-bit authorization number provided by the user. The vendor may also check a data base to see if this was the first use of that authorization number. If the user supplied authorization number matches the authorization number generated by the software vendor, a special password is generated by the software vendor. The password is generated by forwarding an electronic message to a key distribution center 14. The key distribution center 14 using the program number, diskette serial number, and computer number produces a cryptographic key unique to the program and computer. The key distribution center 14 then returns this key to the software vendor. The software vendor, meanwhile, obtains from its data base the file key corresponding to the program number provided by the caller. This key is then encrypted in encryption block 34 with a cryptographic key provided by the key distribution center 14 to generate the requested password. Thus, *Matyas* requires obtaining the password from the software vendor prior to using the software. When the program is loaded on the computer 10, it requests the user to input the password. Thereafter, the password is written by the program in the header record of the file shown in Figs. 2 and 7.

In contrast, the medium personal number unique to each storage medium of the present invention is written on the storage medium before the user receives the storage medium. Additionally, the medium personal number is not created utilizing a combination of the disk number, program number and computer number as is the password taught by *Matyas*. Consequently, *Matyas* teaches only the use of a password and not a medium personal number as recited in applicants' claims. Furthermore, the claimed invention is capable of use on multiple computers while using the same medium personal number. The password taught by *Matyas* is only valid for one computer. Therefore, in order to use the program on the diskette, the user must obtain a second password for use on the second computer. Thus, the password changes for each computer. In contrast, the medium personal number, while unique to the storage medium, does not change when the storage medium is utilized in a new computer. Thus, the medium personal number claimed by applicants is neither taught nor suggested by the use of a password in *Matyas*.

Therefore, applicants request reconsideration and withdrawal of the rejection of claims 1-2, 6-7, 11-12, and 17-18 under 35 U.S.C. § 102(b).

**35 U.S.C. § 103(a)**

Claims 3-5, 8-10, and 13-16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Matyas* discussed above, in view of *Shear* (U.S. Patent No. 4,827,508).

*Shear* is cited for teaching the use of an optical disk or CD-Rom together with teaching using different coding for different files stored on the medium.

*Shear*, however, fails to correct the deficiencies noted above in *Matyas*. Specifically, *Shear* fails to teach a medium personal number that is unique to the storage medium and permits the storage medium to be transferred between different computers. Therefore, applicants request reconsideration and withdrawal of the rejection to claims 3-5, 8-10, and 13-16 under 35 U.S.C. § 103(a).

**Conclusion**

Applicants' remarks have clearly overcome the objections and rejections set forth in the Office Action dated May 19, 2000. Specifically, applicants filing the statement under 37 C.F.R. § 3.73(b) overcomes the objection to the application under 37 C.F.R. § 1.172(a). Applicants will file a supplemental reissue oath/declaration prior to allowance as allowed under M.P.E.P. § 1414 and thus applicants have addressed rejection of claims 1-18 under 35 U.S.C. § 251. Applicants' remarks clearly distinguish claims 1-2, 6-7, 11-12, and 17-18 from the disclosure of *Matyas* and thus overcomes the rejection of these claims under 35 U.S.C. § 102(b). Applicants' remarks in distinguishing the claimed invention from that disclosed in *Matyas* also distinguished claims 3-5, 8-10, and 13-16 from the combination of *Matyas* and *Shear*, and thus overcome the rejection of these claims under 35 U.S.C. §

103(a). Consequently, claims 1-18 are in condition for allowance. Therefore, applicants respectfully request consideration allowance of claims 1-18.

Applicants admit that the application is now in condition for allowance. If the Examiner believes the application is not in condition for allowance, applicants respectfully request that the Examiner contact the undersigned attorney by telephone if it is believed that such contact will expedite the prosecution of the application.

The Commission is authorized to payment for any additional fees which may required with respect to this paper to our Deposit Account No. 01-2300.

Respectfully submitted,

By: MHill
Rustan J. Hill
Registration No. 37,351

ARENT FOX KINTNER PLOTKIN & KAHN, PLLC
1050 Connecticut Avenue, N.W.
Suite 600
Washington, D.C. 20036-5339
Tel: (202) 857-~~6000~~6126
Fax: (202) 638-4810